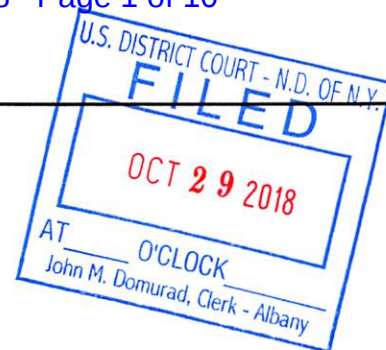


AO 106 (Rev. 04/10) Application for a Search Warrant (Page 1)

UNITED STATES DISTRICT COURT
for the
Northern District of New York



In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))

Case No. 1:18-MJ-647 (CFH)

One (1) Lenovo laptop computer, serial number:)
CB11082195;)

CURRENTLY LOCATED AT THE)
SCHODACK POLICE DEPARTMENT,)
1797 COLUMBIA TURNPIKE,)
CASTLETON, NEW YORK)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property: (identify the person or describe the property to be searched and its given location):

See Attachment A.

located in the Northern District of New York, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252A	Receipt, Transportation, and Possession of Child Pornography

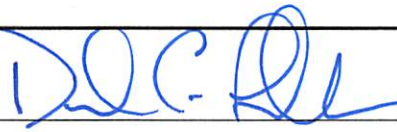
The application is based on these facts:

See attached affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days):

is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

AO 106 (Rev. 04/10) Application for a Search Warrant (Page 2)



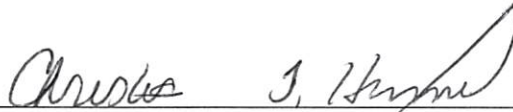
Applicant's signature

FBI Special Agent David C. Fallon

Printed name and title

Sworn to before me and signed in my presence.

Date: October 29, 2018



Judge's signature

City and State: Albany, NY

Hon. Christian F. Hummel, U.S. Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, David C. Fallon, being duly sworn, depose and state:

INTRODUCTION

1. I, David C. Fallon, duly state that I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since May 19, 1991. I am currently assigned to the Albany, NY Division. My experience as an FBI Agent includes being assigned to conduct criminal investigations occurring in the Northern District of New York. I have been a Special Agent of the FBI for over twenty-seven years. I have conducted numerous investigations of computer related crimes including crimes associated with the possession/distribution/production of child pornography and child exploitation using the Internet. I am also a member of the FBI's Child Abduction Rapid Deployment Team with extensive specialty training related to conducting, leading, and managing investigations related to missing and abducted children. I also serve as the case agent for the Albany Division's Child Exploitation Task Force, which targets online child sexual predators and those individuals who trade child pornography. Prior to becoming employed as a Special Agent, I was an attorney licensed to practice law in the State of Rhode Island. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

2. This affidavit is made in support of an application for a warrant to search a Lenovo brand laptop computer, serial number: CB11082195 (“the device”), currently in the custody of the Schodack Police Department, hereinafter SPD, and also described in *Attachment A*.

3. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information for the evidence detailed in *Attachment B* to this application and search warrant, which are items evidencing a violation of Title 18, United States Code, Section 2252A (receipt and possession of child pornography).

4. The device is currently in storage at the Schodack Police Department (SPD), 1797 Columbia Turnpike, Castleton, New York. In my training, experience and in conversation with a representative of the SPD, I know that the device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the device first came into the possession of SPD.

BASIS OF INFORMATION

5. The statements contained in this affidavit are based on my participation in the investigation of this matter, on information I have received from other members of the FBI and SPD. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish

probable cause to believe that evidence of violations of Title 18, United States Code, Section 2252A, as outlined in *Attachment B*, are located within the item, as described above.

OVERVIEW OF INVESTIGATION

6. On October 1, 2018, Jane Doe, a resident of Castleton, N.Y., called 911 to report that she found child pornography on a family laptop used by both her and James McGovern. SPD Patrolman Michael Miller responded to Jane Doe's residence and spoke with her. Patrolman Miller advised your affiant that he spoke with Jane Doe and she advised him that McGovern has been downloading child pornography for several years, and that she finally became sick and tired of it, and that is why she called 911 to report it.

7. Jane Doe then brought Patrolman Miller to the kitchen in her residence and showed him a Lenovo laptop situated on top of the kitchen table. According to Patrolman Miller, Jane Doe opened the Internet browser on the laptop's desktop and navigated to the Download section of the browser. Patrolman Miller observed that the Download folder contained a number of jpeg files which depicted "underage, under-developed girls naked and in sexual positions." Patrolman Miller also advised your affiant that he observed images of underage girls engaged in sexual behavior with what appeared to be semen on their genitalia, faces and stomachs. Jane Doe gave permission for Patrolman Miller to remove the laptop from the residence. Thereafter, Patrolman Miller secured the laptop and brought it to SPD where he placed it into evidence storage.

8. Accordingly, there is probable cause to believe that the device turned over to the SPD contains information and evidence, including but not limited to graphic image files depicting minors engaged in sexually explicit conduct, which, among other things, as

described below, is evidence of violations of Title 18, United States Code, Section 2252A, as more particularly described in *Attachment B*.

FORENSIC EVIDENCE

9. As further described in *Attachment B*, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge

about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

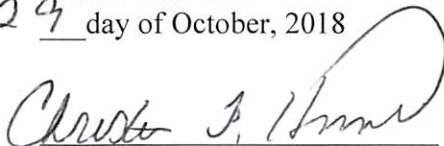
CONCLUSION

10. Based upon the above information, probable cause exists to believe that evidence of violations of Title 18, United States Code, Section 2252A, as outlined in *Attachment B*, of this Affidavit, will be found within the device described above and in *Attachment A*. Accordingly, I respectfully request that this Court issue a search warrant authorizing examination of the contents of the device for the evidence and items described in *Attachment B*.



David C. Fallon
Special Agent
Federal Bureau of Investigation

Sworn to me this
29 day of October, 2018



Hon. Christian Hummel
United States Magistrate Judge

ATTACHMENT A
PROPERTY TO BE SEARCHED

A Lenovo brand laptop computer, serial number: CB11082195, currently in the custody of the Schodack Police Department, 1797 Columbia Turnpike, Castleton, N.Y. ("the device"). This warrant authorizes the forensic examination of the device to identify the electronically stored information described in *Attachment B*.

ATTACHMENT B
ITEMS TO BE SEIZED

Items evidencing violations of Title 18, United States Code, Section 2252A (Receipt, Transportation, and Possession of Child Pornography):

1. All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, and any mechanism used for the receipt or storage of the same, including but not limited to any and all computer passwords, counter-forensic programs, and other data security devices designed to restrict access to, hide, or destroy computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.
2. Any and all documents, records, images, videos, emails, email software, associated email addresses, email address book contents, internet history, browsing history, internet search history, cookies, deleted files, bookmarked and favorite web pages, user typed web addresses, desktop shortcuts, path and file names for files opened through any media and/or image viewing software, anonymizing software, encryption software, chat software, chat files, chat logs, chat names used, peer to peer software, peer to peer files, contact lists, newsgroup postings by the user, IP addresses assigned, access logs, and other evidence pertaining to the receipt, transportation, and possession of images of minor children, including child pornography or child erotica.
3. Records of personal activities relating to the operation and ownership of the media set forth the search warrant, such as contacts, notes (however and wherever written, stored, or maintained), and reference materials.
4. Any records pertaining to accounts held with Internet Service Providers or of Internet use.
5. Records of address or identifying information for users of the device that is the subject of the search warrant, and any names, user IDs, electronic ID numbers, and passwords.
6. Documents and records, including, for example, electronically stored receipts, banking records, bills, statements, telephone records, and other similar indicia of ownership indicating occupation, possession, or control over the device to be searched.
7. Computer records and evidence identifying who the particular user was who transported, downloaded or possessed any child pornography found on the

device, or who searched for, researched, wrote about, or otherwise generated evidence of the items listed in paragraph 1, above (evidence of attribution).